



# Homeland Security

## Daily Open Source Infrastructure Report

### 30 October 2012

#### **Top Stories**

- The supply of gasoline, diesel, and jet fuel into the East Coast almost completely stopped October 29, as Hurricane Sandy forced the closure of two-thirds of the region's refineries, its biggest pipeline, and most major ports. – *Reuters* (See item [1](#))
- U.S. stock markets were to be closed for 2 consecutive days due to weather, NBC News reported October 29. The decision to close financial markets for a second straight day October 30 was made during a call between industry executives and regulators October 29, Reuters said. – *NBC News; Reuters; Associated Press* (See item [9](#))
- Airline and ground transportation systems in three major metropolitan areas shut down as Hurricane Sandy moved closer to the East Coast, CNN reported October 29. More than 10 million public transit commuters were without service. – *CNN* (See item [15](#))
- The South Carolina Department of Revenue's Web site was hacked and millions of Social Security numbers and credit and debit card numbers belonging to approximately 77 percent of South Carolina residents were compromised, WIS 10 Columbia reported October 28. – *WIS 10 Columbia* (See item [28](#))

---

#### **Fast Jump Menu**

##### **PRODUCTION INDUSTRIES**

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

##### **SUSTENANCE and HEALTH**

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

##### **SERVICE INDUSTRIES**

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

##### **FEDERAL and STATE**

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

## **Energy Sector**

1. ***October 29, Reuters*** – (National) **Sandy cuts E. Coast fuel supply; refiners, pipelines shut.** The supply of gasoline, diesel, and jet fuel into the East Coast ground almost to a halt October 29, as Hurricane Sandy forced the closure of two-thirds of the region's refineries, its biggest pipeline, and most major ports. Benchmark New York harbor gasoline futures jumped as much as 11 cents a gallon, with traders fearing that power outages and flooding could leave refiners struggling to restore operations after the broadest storm ever to hit the United States. With Sandy gaining strength as it nears the coast, refinery, pipeline, port, and terminal operators shuttered or reduced operations, increasing the risk that bottlenecks would keep supplies of motor and heating fuel from customers. Colonial Pipeline, the nation's largest oil products pipeline that connects the East Coast to Gulf Coast refiners, said it has shut down lines servicing individual terminals along the Northeastern seaboard. Nearly 70 percent of the region's refining capacity was on track to be idled.  
Source: <http://www.reuters.com/article/2012/10/29/storm-sandy-refining-idUSL1E8LS1OU20121029>
2. ***October 29, WTVF 5 Nashville*** – (Tennessee) **Page Middle, High Schools dismissed due to gas leak.** Students at two Williamson County, Tennessee schools were dismissed October 29 due to a gas leak in the area. A strong gas odor was detected at Page Middle and Page High Schools. The school system proceeded with their evacuation plan as a precaution, and bused 1,7000 students to the Williamson County Ag Center. The gas company turned off the gas, tested and found the leaks, and were attempting to fix them. They said the schools are near a gas company "pickup point" where the rotten egg smell is added. No nearby homes were evacuated, and no one was sickened by the leak. Parents were able to pick up their children at any point, and students were bused back at 1:30 p.m. where parents could get them. Officials said they will make a decision about school October 30.  
Source: <http://www.newschannel5.com/story/19941274/gas-leak-cancels-school-at-page-middle-high-schools>
3. ***October 26, Nextgov*** – (National) **Largest U.S. energy marketing agency used outdated security patches.** The government's largest renewable power transmission agency used a default password to protect its electricity scheduling database and regularly failed to update security software, according to an audit released October 26 by the Energy Department's inspector general (IG). The Western Area Power Administration markets and delivers hydroelectric energy to utilities serving millions of homes and businesses in the Rocky Mountain, Sierra Nevada, Great Plains, and Southwest regions. The agency depends on information technology systems to manage its massive electrical power complex and finances, according to federal officials. Testing uncovered a public-facing server "that was configured with a default username and password," according to the report. "This high-risk vulnerability could have been exploited by an attacker from any Internet connection to obtain unauthorized access to the internal database supporting the electricity scheduling system." Intruders also could have accessed other computer stations at Western's offices and its customers' offices through the same glitch. IG officials did not probe any supervisory control and data

acquisition (SCADA) systems that control electricity flow "because of concerns over the potential impact to operations," the IG wrote. Of the 105 workstations that investigators evaluated, nearly all contained at least one high-risk vulnerability involving software patches. One network server that was running outdated software "could disrupt normal business operations," if a perpetrator performed a "remote code execution" attack to manipulate the server from afar, the report stated. Western also was too generous in granting employees access to its systems. In at least five instances, the agency did not block personnel from computers used for power maintenance and scheduling after they stopped working for the agency.

Source: <http://www.nextgov.com/cybersecurity/2012/10/largest-us-energy-marketing-agency-used-outdated-security-patches/59058/>

For another story, see item [26](#)

[\[Return to top\]](#)

## **Chemical Industry Sector**

4. *October 29, Associated Press* – (Kentucky) **Train derails in Louisville, HAZMAT teams called.** A hazardous materials alert was issued October 29 in southern Louisville, Kentucky, after a train derailed in the area and emitted a strong chemical odor. A MetroSafe spokeswoman said about 20 houses were evacuated because multiple chemicals spilled from the train. The spokeswoman said the train derailed near the Ohio Valley Dragway on Dixie Highway and spilled multiple chemicals including hydrogen chloride and hydrochloric acid. A Level 3 HAZMAT alert, the highest possible, was issued for the area.

Source: <http://www.wbko.com/news/headlines/Train-Derails-in-Louisville-HazMat-Teams-Called--176279891.html?ref=891>

For another story, see item [16](#)

[\[Return to top\]](#)

## **Nuclear Reactors, Materials and Waste Sector**

5. *October 29, Reuters* – (New Jersey; Maryland; Pennsylvania) **Sandy likely to shut at least two NJ nuclear reactors.** At least two major New Jersey nuclear power plants are likely to shut October 29 as Hurricane Sandy makes landfall as a Category 1 storm, and more plants could reduce power as the storm triggers precautionary safety measures, Reuters reported October 29. The nuclear reactors in Sandy's current path include units at Public Service Enterprise Group Inc's (PSEG) 2,332-megawatt (MW) Salem and 1,161-MW Hope Creek plants in New Jersey, which were likely to bear the brunt of the storm before it moves inland. Those plants combined would account for about 19 percent of the State's total electricity capacity, although New Jersey also draws supplies from the whole Pennsylvania, New Jersey, Maryland (PJM) power region. Electricity traders said if Sandy continues on her expected path it was likely PSEG would have to shut the Salem and Hope Creek reactors later October 29, but they

were mixed on whether the storm's winds would still be strong enough to force the shutdown reactors in Pennsylvania and Maryland. A PSEG spokesman said the company would take the Salem and Hope Creek reactors offline if wind speeds reach greater than 74 miles per hour onsite for more than 15 minutes or the river water level reaches 100 feet.

Source: <http://www.reuters.com/article/2012/10/29/us-storm-sandy-utilities-idUSBRE89S0MO20121029>

6. ***October 29, ABC News*** – (National) **Nuclear plants in Sandy's path brace for storm.** The federal government is sending extra inspectors to nine different nuclear power plants in the path of Hurricane Sandy, including Three Mile Island and New York's Indian Point, to make sure the plants are prepared, ABC News reported October 29. All plants already have two inspectors on site equipped with satellite phones. In addition to Indian Point and Three Mile Island, the facilities include the Salem, Hope Creek, and Oyster Creek nuclear plants in southern New Jersey; Peach Bottom and Susquehanna in Pennsylvania; Calvert Cliffs in Maryland; and Millstone in Connecticut. The agency noted that the plants have emergency diesel generators available if off-site power is lost during the storm. "Also, all plants have flood protection above the predicted storm surge," said the NRC, "and key components and systems are housed in watertight buildings capable of withstanding hurricane-force winds and flooding." The NRC will be monitoring the storm from its Incident Response Center in King of Prussia, Pennsylvania, and from the Operations Center at agency's headquarters in Rockville, Maryland. However, its headquarters and Northeast regional office were closed except for emergency personnel. The Oyster Creek and Salem plants are close to where Sandy was expected to make landfall in Delaware and New Jersey late October 29, but their reactors have already been shut down for maintenance, as has the Susquehanna plant in Pennsylvania.

Source: [http://abcnews.go.com/Blotter/nuclear-plants-sandys-path-brace-storm/story?id=17590194#.UI7RnG\\_A\\_9U](http://abcnews.go.com/Blotter/nuclear-plants-sandys-path-brace-storm/story?id=17590194#.UI7RnG_A_9U)

[\[Return to top\]](#)

## **Critical Manufacturing Sector**

7. ***October 29, U.S. Department of Transportation*** – (National) **NHTSA recall notice - BMW 7-Series automatic transmission control module.** BMW is recalling 45,500 model year 2005-2008 7-Series vehicles, equipped with the Comfort Access option and manufactured August 23, 2004, through July 24, 2008. The affected vehicles have an electronic key and an electronic connection between the gear shifter and the transmission (shift-by-wire) that automatically shifts the transmission to Park when the driver presses the Start/Stop button to shut down the engine. If the driver presses the engine Start/Stop button 2 or 3 times within a short time interval, the system may shift the transmission to Neutral rather than Park. If using the electronic key (Comfort Access mode), there would be no protection from the ignition interlock that prevents key removal if the vehicle is not in Park. If the driver exits the vehicle with the transmission in Neutral and the parking brake is not applied, the vehicle may rollaway. Unattended rollaway incidents often result in a crash or cause injury to pedestrians

attempting to stop or enter the vehicle or to other bystanders in the path of the vehicle. BMW will notify owners beginning in November 2012, but will not have revised software available to remedy the vehicles until March 2013.

Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl\\_ID=12V502000&summary=true&prod\\_id=204671&PrintVersion=YES](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V502000&summary=true&prod_id=204671&PrintVersion=YES)

[[Return to top](#)]

## **Defense Industrial Base Sector**

8. ***October 29, Global Security Newswire*** – (New Mexico) **NNSA pledges to fix Los Alamos plutonium site defense system.** The Presidential administration said it would work to eliminate technical flaws in a developmental protective mechanism for the country's sole facility capable of producing key nuclear-bomb explosion initiator components, the Associated Press reported October 26. Defensive technology under preparation to guard the Technical Area 55 plutonium site continue to suffer from significant malfunctioning, the Los Alamos National Laboratory in New Mexico verified. Officials previously announced plans to indefinitely defer completion of the 7-year-old project that has absorbed \$213 million in funding, according to earlier reporting. The National Nuclear Security Administration would dispatch specialists to the laboratory "to examine the financial and management issues that led us to this point," a spokesman for the agency said. Separate controversies focused on the potential for radioactive material to escape from the Los Alamos laboratory's aging PF-4 plutonium site, and on the spiking expense of the facility's Chemistry and Metallurgy Research Replacement Project. The Presidential administration is seeking to delay that initiative.

Source: <http://www.nti.org/gsn/article/nnsa-pledges-fix-lanl-plutonium-site-defenses/>

[[Return to top](#)]

## **Banking and Finance Sector**

9. ***October 29, NBC News; Reuters; Associated Press*** – (New York; National) **Hurricane Sandy to keep stock markets shuttered Tuesday.** For the first time since the Great Blizzard of 1888, U.S. stock markets were to be closed for 2 consecutive days due to weather, NBC News reported October 29. The decision to close financial markets for a second straight day October 30 was made during a call between industry executives and regulators October 29, Reuters said. The New York Stock Exchange (NYSE) and the Nasdaq Stock Market both said they intended to remain closed for business a second day. The bond market will also remain closed. The NYSE shuttered its operations October 29 as Hurricane Sandy neared landfall on the East Coast, bringing about the first unplanned shutdown since the September 2001 terrorist attacks. "We intend to re-open our U.S. markets on Wednesday ... conditions permitting; updates will be provided tomorrow," the NYSE said in an email. All major U.S. stock and options exchanges were closed October 29. Options and other exchange-based derivatives would remain closed October 30 due to the storm. There had been plans to allow

electronic trading to go forward on the New York Stock Exchange October 29, but with all mass transit shut down in and out of New York City's Manhattan area, the risks were determined to be too great. A number of major U.S. companies postponed quarterly earnings as financial markets shut down.

Source: [http://marketday.nbcnews.com/\\_news/2012/10/29/14778477-hurricane-sandy-to-keep-stock-markets-shuttered-tuesday?lite](http://marketday.nbcnews.com/_news/2012/10/29/14778477-hurricane-sandy-to-keep-stock-markets-shuttered-tuesday?lite)

10. **October 29, The Register** – (Texas; National) **Hackers crack Texan bank, Experian credit records come flooding out.** Hackers managed to get login credentials for Experian's credit scoring reports after they broke into the systems of Abilene Telco Federal Credit Union in Abilene, Texas, in 2011, The Register reported October 29. Crooks gained access to the bank's systems after hacking into an employee's computer. The September 2011 breach allowed the hackers to get their hands on login credentials for the bank's account with Experian, exposing the details of millions to potential snooping in the process. A subsequent audit revealed that the attackers had used the compromised account to download credit reports on 847 people, obtaining Social Security numbers, dates of birth, and financial data on individuals across the U.S. who had never held an account with the small Texas bank. The breach is one of 86 incidents that have exposed data stored by credit reference agencies to snooping since 2006. Hackers have obtained this information not by going after the credit reference agencies directly but by targeting banks, auto-loan firms, data brokers, police departments, and other organizations that have access to the sensitive information, which can be used by identity thieves to establish lines of credit under false names.

Source: [http://www.theregister.co.uk/2012/10/29/credit\\_report\\_data\\_breach\\_worries/](http://www.theregister.co.uk/2012/10/29/credit_report_data_breach_worries/)

11. **October 27, Imperial Valley News** – (California; Nevada) **Fourteen charged in million-dollar 'gone in 60 seconds' bank fraud.** Fourteen individuals were charged following a FBI-led investigation into the theft of over \$1 million from Citibank using cash advance kiosks at casinos located in southern California and Nevada. According to an indictment unsealed October 26, the defendants stole the money by exploiting a gap which required multiple withdrawals all within 60 seconds in Citibank's electronic transaction security protocols. According to court documents, a defendant recruited conspirators who were willing to open multiple Citibank checking accounts. He then supplied his co-defendants with "seed" money, which was deposited into the recently opened accounts. After the money was deposited into the checking accounts, he and his conspirators would travel to nearly a dozen casinos in California and Nevada. When inside the casino, the conspirators used cash advance kiosks at casinos to withdraw several times the amount of money deposited into the accounts, by exploiting the Citibank security gap they discovered. As part of the alleged scheme, the defendants kept both their deposits and withdrawals under \$10,000 in order to avoid federal transaction reporting requirements and conceal their fraud.

Source: <http://www.imperialvalleynews.com/index.php/news/california-news/2126-fourteen-charged-in-million-dollar-gone-in-60-seconds-bank-fraud.html>

12. **October 27, Bay Area Newsgroup** – (California) **Campbell: 'Beanie Bandit' arrested in connection with six South Bay bank robberies.** A man suspected of being the "Beanie Bandit" who robbed six South Bay area, California banks was arrested October

26 after officers tracked him down and stopped his car, police said. Campbell police arrested the man after finding money and clothing in his home that was seen in the surveillance videos. He is suspected of robbing the six bank branches between August 24 and October 12. Two banks in Campbell, two in Sunnyvale, one in San Jose, and one in Los Gatos were hit. Sunnyvale police said that during the October 12 robbery at a Bank of America branch, the robber had given the teller a note stating that he was armed with a gun, but no weapon was seen.

Source: [http://www.mercurynews.com/campbell/ci\\_21869883/campbell-beanie-bandit-arrested-connection-six-south-bay](http://www.mercurynews.com/campbell/ci_21869883/campbell-beanie-bandit-arrested-connection-six-south-bay)

13. ***October 26, U.S. Securities and Exchange Commission*** – (California; National) **SEC charges Silicon Valley executive for role in Galleon insider trading scheme.** The Securities and Exchange Commission (SEC) October 26 charged a Saratoga, California former senior executive at a Silicon Valley technology company for illegally tipping a convicted hedge fund manager with nonpublic information that allowed the Galleon hedge funds to make nearly \$1 million in illicit profits. The SEC alleges that the former senior executive tipped the hedge fund manager in December 2006 with confidential details from internal company reports indicating that Xilinx Inc. would fall short of revenue projections it had previously made publicly. The tip enabled the hedge fund manager to engage in short selling of Xilinx stock to illicitly benefit the Galleon funds. The executive tipped the manager, who was a close friend, at a time when the executive had his own substantial investment in Galleon funds and was in discussions with the manager about prospective employment at Galleon. The executive was hired at Galleon in May 2007. The executive agreed to pay more than \$1.75 million to settle the SEC's charges.

Source: <http://www.sec.gov/news/press/2012/2012-216.htm>

14. ***October 26, U.S. Securities and Exchange Commission*** – (Colorado) **SEC charges Denver-based insurance executive with insider trading.** The Securities and Exchange Commission (SEC) October 26 charged an insurance company CEO with insider trading based on confidential information he obtained in advance of a private investment firm acquiring a significant stake in a Denver-based oil and gas company. The SEC alleges that the CEO learned from a Delta Petroleum Corporation insider that Tracinda was planning to acquire a 35 percent stake in Delta Petroleum for \$684 million. The CEO subsequently purchased Delta Petroleum stock and highly speculative options contracts. He tipped several others, encouraging them to do the same, including a pair of relatives. After Tracinda's investment was publicly announced, Delta Petroleum's stock price shot up by almost 20 percent. The CEO and his tippees made more than \$161,000 in illegal trading profits. The U.S. Attorney's Office for the District of Colorado also announced a parallel criminal action against the CEO.

Source: <http://www.sec.gov/news/press/2012/2012-217.htm>

[[Return to top](#)]

## **Transportation Sector**

15. *October 29, CNN* – (National) **Sandy snarls travel along the East Coast.** Airline and ground transportation systems in three major metropolitan areas shut down as Hurricane Sandy moved closer to the East Coast, CNN reported October 29. More than 10 million public transit commuters were without service. There were more than 8,000 flight cancellations as a result of the hurricane, according to FlightAware.com. Some 1,300 domestic and international flights were canceled October 28, according to FlightAware, with more than 6,800 October 29 flights canceled. More than 2,500 October 30 flights were already canceled, according to FlightAware. That number was expected to grow. US Airways announced the cancellation of all its October 30 operations at Philadelphia, Washington, Boston, and New York City airports. All October 29 operations at New York and New Jersey's three major metro airports were canceled, according to the Port Authority of New York and New Jersey. The majority of flights were also canceled out of Dulles International and Reagan National airports in the Washington, D.C. area, according to Metropolitan Washington Airports Authority. All October 29 flights out of Philadelphia International Airport were also canceled, an airport spokeswoman said. Flights were suspended at Connecticut's Bradley International Airport as well. New York's ubiquitous subway and bus services stopped October 28, and it was unknown when service would be restored. The area's Metropolitan Transit Authority Service, which also operates the Long Island Rail Road, Metro-North Railroad, serving Westchester and Connecticut, and the city's Staten Island Railway, suspended service on those three train lines. In New Jersey, the suspension of all NJ Transit bus, rail, light rail, and Access Link service was complete as of October 29. The Washington Metro system remained idle, and it was unclear when bus service and rail service would be restored, the Washington Metropolitan Area Transit Authority said. The 770,000 riders who use public transit each day in the Philadelphia area were also impacted. Amtrak said it was canceling almost all services on the eastern seaboard October 29. Bus lines connected to those trains were also canceled.

Source: <http://www.cnn.com/2012/10/28/travel/tropical-weather-transportation/index.html>

16. *October 29, Los Angeles Times* – (Delaware; New Jersey; New York) **Nation's third-busiest cargo port evacuated, closed as storm hits.** The nation's third-busiest cargo container seaport was evacuated and closed because of Hurricane Sandy, officials from the Port Authority of New York-New Jersey said. They made the announcement in a statement, adding that the evacuation was completed by October 29. The New York-New Jersey seaport is a vital economic engine that handled more than 5.5 million cargo containers in 2011. It ranked as the third-busiest container port in the United States. Also closed was the port of Wilmington, Delaware, which stopped operations October 29. Major businesses were also being affected. DuPont closed its headquarters in Wilmington, Delaware, and some of its laboratories and factories. Dow Chemical shut down its facilities in the Delaware Valley.

Source: <http://www.latimes.com/business/money/la-fi-mo-ports-closed-20121029,0,3386069.story>

17. *October 29, WZVN 7 Fort Myers* – (Michigan) **Driver wounded in interstate shooting.** A motorist driving along Interstate 96 was shot and wounded October 27 in the latest in a string of shootings in southeastern Michigan. A Livingston County sheriff said the Delton man was taken to the hospital for a gunshot wound in the left buttock area by a bullet that came through the door. He was listed in stable condition at a hospital. The sheriff said shots were fired into another car earlier, but the two people inside were not hurt. A specially-formed task force with dozens of investigators has been working to solve 24 reported shootings along the interstate, or near it, in Ingham County, Oakland County, Livingston County, and Shiawassee County. Ten of the incidents happened in Wixom alone. No one was hurt in any of the previous shootings. Source: [http://www.abc-7.com/story/19941973/\\_driver-wounded-in-interstate-shooting](http://www.abc-7.com/story/19941973/_driver-wounded-in-interstate-shooting)

18. *October 29, Associated Press* – (New York) **NYC waters rise to Irene levels before superstorm.** Waves splashed over the sea walls at the southern tip of Manhattan in New York City, already at Hurricane Irene levels October 29 hours before the worst of the storm was to hit the city with a wall of water that could reach 11 feet. The Governor closed two key tunnels to downtown Manhattan and the city canceled schools for a second day after shutting its mass transit system and ordering hundreds of thousands of people to leave their homes ahead of Hurricane Sandy's storm surge. Minor flooding had affected some Long Island fishing villages and coastal towns, New York's Rockaway peninsula, and a highway on the east side of Manhattan, officials said. More than 20,000 customers, mostly in Long Island, had lost power; most of the city's 3,600 outages were in Brooklyn. The floor of the New York Stock Exchange was deserted in its first unplanned shutdown since the September 11, 2001, terror attacks. The Governor scheduled the close the flood-prone Brooklyn Battery and Holland Tunnels, later October 29. He also deployed National Guard troops to the city and Long Island. Consolidated Edison weighed the possibility of shutting down power in parts of lower Manhattan to protect equipment. Broadway shows were canceled for October 28 and October 29. One small hospital was being evacuated, while several others were moving patients to higher floors. Source: <http://online.wsj.com/article/AP03cbe7a14aba48469943103489e10e83.html>

For more stories, see items [4](#) and [27](#)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

19. *October 29, Carroll County Times* – (Maryland) **USPS: Storm may impact mail delivery.** The U.S. Postal Service prepared for the arrival of Hurricane Sandy by advising customers that normal service operations in the path of the storm may be affected in the event of unsafe conditions such as high winds, flooding, or impassable roads, according to a news release. Regular postal operations were expected to be in effect for October 29. Depending on local conditions, some Post Offices may temporarily close their lobbies as Hurricane Sandy makes landfall. The Postal Service will make plans to suspend services in the event a mandatory evacuation order is issued by local, State, or federal emergency management officials. Customer service

operations in any area covered by a mandatory evacuation order will be suspended, including mail processing, mail delivery, scheduled collection of mail from mail collection boxes, bulk mail acceptance, Post Office box service and retail Post Office lobby services. Drop shipment appointments for commercial mailers will also be suspended at closed facilities. USPS would provide updates on the latest information on service updates on their Web site.

Source: [http://www.carrollcountytimes.com/emergency/usps-storm-may-impact-mail-delivery/article\\_c87e5d17-365c-5417-9475-be17e23df2a3.html](http://www.carrollcountytimes.com/emergency/usps-storm-may-impact-mail-delivery/article_c87e5d17-365c-5417-9475-be17e23df2a3.html)

[[Return to top](#)]

## **Agriculture and Food Sector**

20. ***October 29, U.S. Food and Drug Administration*** – (Kentucky; Virginia; Tennessee) **Schoep's Ice Cream Company issues allergy alert on undeclared allergen in Kays Classic Vanilla Bean Ice Cream.** Schoep's Ice Cream Company of Madison, Wisconsin, alerted customers that, because of a packaging error, Kays Classic Vanilla Bean Ice Cream contains an undeclared allergen, the U.S. Food and Drug Administration announced in an update October 29. The recalled product is in 48-ounce container, UPC 0-87848-13021, and has a best-if-used-by date of February 28, 2014. The product was shipped to Food City and Super Dollar stores in Kentucky, Virginia, and Tennessee.  
Source: <http://www.fda.gov/Safety/Recalls/ucm326106.htm>
21. ***October 27, Food Safety News*** – (National) **CDC: 22 Illnesses and 4 deaths now linked to Listeria cheese.** Two more cases were added to the multi-State outbreak of listeriosis linked to imported Frescolina Marte brand ricotta salata cheese, according to the Centers for Disease Control and Prevention (CDC). As of October 26, the CDC said a total of 22 persons infected with the outbreak-associated strain of Listeria monocytogenes were reported from 13 States and the District of Columbia. Of the known cases, 20 people were hospitalized; four deaths were reported. Listeriosis contributed to at least two of these deaths, according to the CDC's update. The agency also said that one fetal loss was reported.  
Source: <http://www.foodsafetynews.com/2012/10/cdc-22-illnesses-and-4-deaths-linked-to-listeria-cheese/>
22. ***October 25, U.S. Food and Drug Administration*** – (National) **Bumble Bar, Inc. recalls Gluten Free Cafe Chocolate Sesame Bars and Gluten Free Cafe Cinnamon Sesame Bars due to possible health risk associated with Sunland Inc. peanut products.** Bumble Bar recalled certain lots of Gluten Free CafÃ© Chocolate Sesame Bars and Gluten Free CafÃ© Cinnamon Sesame Bars associated with Sunland Inc. peanut products because they are potentially contaminated with Salmonella, the U.S. Food and Drug Administration announced in an update October 25. The recalled products were distributed nationwide from June 2011 to October 2012. The products were shipped primarily to retail stores and were also available through Internet orders.  
Source: <http://www.fda.gov/Safety/Recalls/ucm325868.htm>

[[Return to top](#)]

## **Water Sector**

23. *October 29, State Island Advance* – (New York) **Staten Island businesses, homes lose water after main break in New Springville section.** Two water main breaks at Nome and Richmond avenues in New Springville, New York, left 20 businesses and 15 single-family residences without water October 29. There was a 12-inch break at Nome Avenue, said a city Department of Environmental Protection (DEP) spokesman. There was also a secondary 8-inch break in the same vicinity. DEP crews roped off a hole in the ground with orange tape and cones. "Crews are excavating down to the break and will commence repairs once they get down," the spokesman said. There was no estimate as to when the water would be turned back on.

Source:

[http://www.silive.com/westshore/index.ssf/2012/10/staten\\_island\\_businesses\\_homes.html](http://www.silive.com/westshore/index.ssf/2012/10/staten_island_businesses_homes.html)

[[Return to top](#)]

## **Public Health and Healthcare Sector**

24. *October 29, American Medical News* – (National) **Investigation faults handling of Medicare patient data breaches.** In October, the Department of Health and Human Services' Office of the Inspector General (OIG) published a report of its investigation of Centers for Medicare & Medicaid Services' management of a database of Medicare identification numbers, for patients and physicians, which were compromised because of a breach. The report found that Medicare was not doing enough to mitigate damages caused when a Medicare patient's identification is stolen. The OIG found a need for better management of the database and consistency in how Medicare contractors use the database to catch and prevent fraud. The lack of consistency could cause a disruption in payments to physicians and other health care organizations that treat and provide medical supplies to Medicare patients. The OIG examined 14 breaches affecting 13,755 beneficiaries that occurred between September 23, 2009, when the notification rules under the economic stimulus package went into effect, and December 31, 2011. Of the 14 breach cases, the OIG found that: Notification was not made within the required 60 days in seven cases; Notification did not include a description of the breach investigation, loss mitigation, and protection against further breaches in six cases; Notification did not include when breaches occurred or were discovered in seven cases; Notification did not include the breached information, contact procedures, or steps to protect from harm in three cases.

Source: <http://www.ama-assn.org/amednews/2012/10/29/bisb1029.htm>

25. *October 29, Associated Press* – (Rhode Island) **RI has 1st case of fungal meningitis in outbreak.** Rhode Island health officials reported the State's first case of fungal meningitis October 29 in a nationwide outbreak linked to steroid injections prepared by a Massachusetts pharmacy. The Rhode Island Department of Health said a woman was hospitalized and receiving treatment. The department said she received a spinal

injection at Ocean State Pain Management of Woonsocket September 22. Ocean State Pain Management and New England Anesthesiology were the two Rhode Island facilities that received the suspect medications from New England Compounding Center. The health department said 266 people received injections from 3 affected lots. Source: <http://www.timesunion.com/news/article/RI-has-1st-case-of-fungal-meningitis-in-outbreak-3990547.php>

For another story, see item [18](#)

[[Return to top](#)]

## **Government Facilities Sector**

26. *October 29, Kennebec Journal* – (Maine) **Wells officials urge evacuation as Sandy nears.** As Hurricane Sandy approached Maine, with seas expected to produce 25-foot-waves and winds gusts up to 60 miles per hour, the town of Wells advised residents to evacuate homes and businesses in coastal and low-lying areas, the Kennebec Journal reported October 29. The town of Wells said high winds would likely cause downed trees and limbs, as well as cut power. Travel after dark was discouraged. The town advised all businesses and homes east of Route 1 to voluntarily evacuate. No local shelter would be opened. A spokesman for Central Maine Power Co., said 3,350 customers were without power in York and Cumberland counties in towns ranging from Harpswell and Kennebunkport to Brunswick and North Berwick. A handful of schools have announced early release days for students. Portland schools will close one hour early and all after-school and evening activities were canceled. The Governor signed a limited-emergency declaration that allowed Central Maine Power Co. to call in power crews from New Brunswick, Canada. The declaration allowed those crews to exceed the number of hours they are allowed to drive. Some of the crews arrived October 28 in Augusta.

Source: [http://www.kjonline.com/news/sandy-set-to- - -thrash-maine\\_2012-10-29.html](http://www.kjonline.com/news/sandy-set-to- - -thrash-maine_2012-10-29.html)

27. *October 29, Baltimore Sun* – (Maryland) **Ocean City, inundated with flooding, awaits storm's worst.** Ocean City, Maryland, passed its first test of Hurricane Sandy October 29 as the morning high tide and a 7-foot storm surge covered downtown areas and the bayside shoreline with up to 4 feet of water. However the worst was to come, with the storm still on its way and another high tide. The storm surge was already the worst the town has seen since Hurricane Gloria in 1985. So far, no injuries, deaths, or close-call rescues have been reported, town officials said. Conditions were becoming increasingly treacherous, with police halting traffic south of the Route 90 Bridge. In a press conference, the mayor urged residents to stay indoors to ride out the storm. With no public safety crises, much attention in the town and among media focused on the fishing pier at the southern end of the boardwalk. Many of the pilings along the last 150 feet or so of the pier buckled in the heavy surf, with the waves dismantling most of the structure except for the portion over the shoreline. Waves crashed over bulkheads on the town's western shores, covering bayside parking lots and roads with as much as a few feet of water. Two shelters were opened in Ocean City, at the Convention Center

and Northside Park, where residents could wait before being transferred to a Worcester County shelter at Stephen Decatur High School in Berlin. Downtown, floodwaters have reached about 3 to 4 feet, the mayor said. About 200 downtown residents chose to remain in their homes despite a mandatory evacuation south of 17th Street, the town police chief said.

Source: <http://www.baltimoresun.com/news/weather/weather-blog/bs-md-ocean-city-hurricane-impact-20121029,0,3658276.story>

28. *October 28, WIS 10 Columbia* – (South Carolina) **Millions of South Carolinians' Social Security numbers stolen from State agency.** The South Carolina Department of Revenue's Web site was hacked and millions of social security numbers and credit and debit card numbers belonging to approximately 77 percent of South Carolina residents were compromised, WIS 10 Columbia reported October 28. State officials revealed that someone in a foreign country gained access to the Web site and a server was breached for the first time in late August. 387,000 credit and debit card numbers and 3.6 million Social Security numbers were exposed. The Social Security numbers were unencrypted. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under credit card industry standards, officials said. However, approximately 16,000 were unencrypted and exposed. Officials found out about the breach October 10. October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made August 27. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions were uncovered. October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured. The breach potentially affects anyone who has paid taxes in South Carolina since 1998.

Source: <http://www.wbtv.com/story/19926154/social-security-breach-nikki-haley-south-carolina-credit-cards-hacker>

For more stories, see items [18](#) and [39](#)

[\[Return to top\]](#)

## **Emergency Services Sector**

29. *October 29, Roanoke Times* – (Virginia) **Virginia fire station sustains damage during blaze.** Fire destroyed a brick commercial structure in Fieldale, Virginia, October 27, and scorched the building housing the fire department next door, a fire official said. Between 40 and 50 firefighters from 6 or 7 companies fought to save the structure for nearly 4 hours, but were hampered by fallen live electrical lines and a temporary shortage of water, said the chief of the Fieldale Fire Department. He said the two-story commercial building was 90 percent destroyed. The Fieldale Fire Department building had flame damage on the outside and smoke damage inside. Firefighters initially relied on a hydrant that could not produce enough water, forcing crews to drive tankers and engines several miles to access another water line, the chief said. Crews controlled the blaze by October 28.

Source: <http://www.firehouse.com/news/10821038/virginia-fire-station-sustains-damaged-during-blaze>

30. *October 29, Vallejo Times-Herald* – (California) **California Highway Patrol Vallejo dispatch center evacuated after fire.** A computer console inside the California Highway Patrol's (CHP) Vallejo dispatch center caught fire October 28, prompting an evacuation and temporary closure of the building. The console at the dispatch center overheated and caught fire, activating the building's sprinkler system, which quickly put out the blaze, an officer said. Everyone inside the building was evacuated as a safety precaution and the dispatch center was closed. Dispatchers in the CHP's Sacramento and Monterey offices fielded 9-1-1 calls that would normally come to the Vallejo office, and non-emergency calls were being handled by other CHP area offices, the officer said. An estimate of when the dispatch center would reopen was not immediately available October 29.

Source: [http://www.timesheraldonline.com/news/ci\\_21880699/california-highway-patrol-vallejo-dispatch-center-evacuated-after](http://www.timesheraldonline.com/news/ci_21880699/california-highway-patrol-vallejo-dispatch-center-evacuated-after)

31. *October 29, Los Angeles Times* – (California) **Fake mayday calls in O.C. send Coast Guard scrambling.** U.S. Coast Guard officials are trying to track down a man who has reported several fake distress calls in California regarding sinking ships, wasting time and money on rescue efforts, the Los Angeles Times reported October 29. Coast Guard officials said the fake distress calls divert help from people who really need it. During the week of October 22, a man that the Coast Guard tracked to Orange County, California made six calls over the radio. He has prompted two attempted rescues and said things like, "Mayday, mayday, my dog ate my homework," before he claims he is drowning or had some sort of accident. In the last hoax call October 26, the man said his boat was sinking in Newport Harbor. The Coast Guard deployed a vessel that costs \$2,600 per hour and a helicopter that runs more than \$8,600 per hour. In all, the 12 1/2-hour search cost taxpayers about \$50,000, exhausted resources and, according to officials, potentially put other boaters at risk. Now investigators are trying to locate the man who is making the bogus calls.

Source: <http://latimesblogs.latimes.com/lanow/2012/10/fake-mayday-calls-in-oc-send-coast-guard-scrambling.html>

32. *October 25, Associated Press; KTUU 2 Anchorage* – (Alaska) **Correctional officer attacked by inmates at Seward Prison.** A correctional officer and two inmates at a maximum-security State prison in Seward, Alaska, were injured October 24 when a group of inmates assaulted the officer, according to Alaska State Troopers. According to an October 25 AST dispatch, troopers in Crown Point were notified of the incident at the Spring Creek Correctional Center which began when the officer was in an inmate housing area and one inmate attacked him. The Alaska Department of Corrections said the officer was able to call for help. He was subsequently treated and released from a Seward medical facility. An AST spokesperson said no charges have yet been filed in the incident. The incident remains under investigation.

Source: <http://www.ktuu.com/news/correctional-officer-attacked-by-inmates-at-seward-prison-102512,0,5464673.story>

For more stories, see items [18](#) and [39](#)

[[Return to top](#)]

## **Information Technology Sector**

33. *October 29, Help Net Security* – (International) **Privacy-invading module found in thousands of apps on Google Play.** An advertising module embedded into over 7,000 "free" fake versions of legitimate Android applications that can be found on Google Play is actively harvesting personal and mobile use information from unsuspecting users, warned a Trend Micro senior threat researcher. She detected one such app after downloading by mistake a fake Flash Player from Google's official Android market and getting warned about its malicious nature by her company's own mobile security app. After consulting with a colleague from the Mobile Application Reputation team, she discovered the extent of the problem: apart from pushing ads onto the users, the adware module inside the app also sends information such as device ID, OS version, IP address, and the user's phone number, GPS location, account information, calendar, and browser bookmarks to the servers of the company that created the module. This particular ad module compromises the users' privacy and their devices' usability. It was found in over 7,000 free apps offered on Google Play. "80% of them are still available, and at least 10% of them have been downloaded more than one million times," the researcher warned, and added that the Web of Trust community believes the company that created the module is also involved in phishing and scamming users.  
Source: <http://www.net-security.org/secworld.php?id=13860>
34. *October 29, Help Net Security* – (International) **Malware authors turn to simpler detection evasion techniques.** Symantec researchers discovered two new, less-technical approaches malware developers are using to evade automated threat analysis. The first consists of making malware run only if it detects mouse movement or clicking. The second involves inserting delays between the execution of the various malware subroutines. The rationale behind the first test is that automated threat analysis systems do not use the mouse, while regular computer users do. The lack of this movement signals to the malware that it is probably being run in a sandbox. The rationale behind the subroutine execution delays — often spanning over 20 minutes for each — is that given the number of files the system must test, it usually spends only a small amount of time on each file, and chances are the file will be categorized as harmless and discarded before the first subroutine is even run.  
Source: [http://www.net-security.org/malware\\_news.php?id=2307](http://www.net-security.org/malware_news.php?id=2307)
35. *October 29, The H* – (International) **Ubuntu 11.04 reaches its end of life.** An Ubuntu release manager announced that Ubuntu 11.04, code-named "Natty Narwhal," reached its end of life October 28. This means that no new updates, including security updates and critical fixes, will be made available for version 11.04 of Canonical's Linux distribution. Released in April 2011, Natty Narwhal was based on the 2.6.82.2 Linux kernel and was the first version of Ubuntu to replace the GNOME Shell with Unity as its default desktop environment. Firefox 4.0, version 3.3.2 of the LibreOffice productivity suite, and Banshee 2.0 were among the bundled default applications. Users

still running Ubuntu 11.04 are advised to upgrade to version 11.10 "Oneiric Ocelot" or later in order to continue receiving updates. Those wanting to upgrade to the current Long Term Support edition, Ubuntu 12.04, or the most recent standard release, Ubuntu 12.10 "Quantal Quetzal," will need to upgrade in multiple steps, first upgrading to 11.10 and then the subsequent versions.

Source: <http://www.h-online.com/security/news/item/Ubuntu-11-04-reaches-its-end-of-life-1738365.html>

36. *October 27, Softpedia* – (International) **Users lured to Blackhole exploit kit with bogus 'Your Photos' LinkedIn emails.** According to Sophos experts, one of the latest plots by cybercriminals to lure users to a Blackhole exploit kit-infested Web site involves sending out fake LinkedIn emails entitled "Your Photos" in an attempt to trick them into opening an attached .htm file. The notification reads: "Hi, I have attached your photos to the mail (Open with Internet Explorer)." Once the file, called "Image\_DIG[random number].htm" is opened, a "please wait a moment" message is displayed. In the meantime, in the background, the victim is redirected to a Blackhole exploit Web site that is designed to serve malware. The malicious .htm file is detected as Mal/JSRedir-M.

Source: <http://news.softpedia.com/news/Users-Lured-to-BlackHole-Exploit-Kit-With-Bogus-Your-Photo-LinkedIn-Emails-302569.shtml>

37. *October 27, The H* – (International) **Critical security holes closed in Firefox 16 and Thunderbird 16.** Mozilla released a Firefox 16.0.2 update for its browser to close recently discovered critical security holes. Three problems, assigned CVE-2012-4194, CVE-2012-4195, and CVE-2012-4196 were addressed in the updates. The flaws also affect Thunderbird 16 to a more limited extent, but a Thunderbird 16.0.2 update was released. Enterprise ESR versions of the browser and email client are also affected; a 10.0.10 update for Firefox ESR and Thunderbird ESR were also released along with a 2.13.2 update of SeaMonkey. The flaws are centered on the Location object, which now has its security increased. A researcher discovered that the true value of window.location could be shadowed which could have enabled a cross-site-scripting (XSS) attack in conjunction with some plugins. A Mozilla security researcher found that using CheckURL on window.location could be forced to return the wrong calling document, also enabling an XSS attack; there was also a possibility of arbitrary code execution via any add-on that interacted with page content. Finally, a researcher from the PROSECCO research team at INRIA found that it was possible to inject properties into the Location object, exposing it to cross-origin reading.

Source: <http://www.h-online.com/security/news/item/Critical-security-holes-closed-in-Firefox-16-and-Thunderbird-16-1737891.html>

## Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto:sos@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

[[Return to top](#)]

## **Communications Sector**

Nothing to report

[[Return to top](#)]

## **Commercial Facilities Sector**

38. ***October 29, WFAA 8 Dallas-Fort Worth*** – (Texas) **Pastor killed in assault at Forest Hill church.** A pastor was fatally beaten with a guitar in an assault at the Greater Sweethome Missionary Baptist Church October 29 in Forest Hill, Texas. The unidentified suspect in the assault was pronounced dead after officers used a taser to subdue him, Forest Hills police said. The incident began with the suspect crashing into the side of the church and then assaulting two people, including the pastor, MedStar reported. Another woman was stopped by police after she jumped over crime scene tape and attempted to run towards the crime scene.  
Source: [http://www.wfaa.com/news/local/Report-Pastor-killed-in-attack-at-Fort-Worth-church-176292691.html?hpt=ju\\_bn5](http://www.wfaa.com/news/local/Report-Pastor-killed-in-attack-at-Fort-Worth-church-176292691.html?hpt=ju_bn5)
39. ***October 29, WCAU 10 Philadelphia*** – (New Jersey) **Parts of Atlantic Co. under 5 feet of water: Governor.** Parts of Atlantic County, New Jersey, were under 5 feet of water and most of Atlantic City was flooded, according to the Governor, WCAU 10 Philadelphia reported October 29. There was significant flooding in Cape May and Ocean Counties and several rescues were underway on New Jersey's barrier islands. At a news conference, the Governor said everyone who ignored the orders to evacuate made a bad decision and are now putting emergency responders in danger. The worst of the flooding was expected late October 29 when the heaviest rain move in just before Hurricane Sandy makes landfall around midnight. It will also be high tide. "When it comes in tonight, we can't rescue you," said the Governor. 800 people have been evacuated from Atlantic City and are staying in area shelters. However the governor said that only 50 percent of many towns were evacuated in Atlantic and Ocean Counties  
Source: <http://www.nbcphiladelphia.com/news/local/Parts-of-Atlantic-Co-Under-5-Feet-of-Water-Christie-176277881.html>

For more stories, see items [18](#), [23](#), and [26](#)

[[Return to top](#)]

## **National Monuments and Icons Sector**

Nothing to report

[[Return to top](#)]

## **Dams Sector**

40. *October 29, Boston.com* – (Massachusetts) **Water in Cohasset crashes over sea wall; power restored to most of town.** Hurricane Sandy brought waves crashing over the sea wall in Cohasset, Massachusetts, October 29 and police closed several roads due to flooding and rocks being carried by the water. In a phone interview, the town administrator said he was standing at the harbor to watch the water crest but said that there should not be a need for evacuations. The town lowered Jacobs Meadow and Treats Pond about 2 feet last week to help absorb excess water, but officials are still anticipating additional flooding. “We have areas prone to flooding so we’re in watch mode right now,” he said. He added that the town made about 4,000 reverse 9-1-1 calls to residents October 28 and about 3,000 of those were picked up by residents still at home. Now, primary communication is being done through the police department’s Facebook page. The following roads have been closed so far: Jerusalem Road, Bow Street, parts of Atlantic Avenue near the causeway, and Rocky Beach.

Source:

[http://www.boston.com/yourtown/news/cohasset/2012/10/water\\_in\\_cohasset\\_crests\\_over.html](http://www.boston.com/yourtown/news/cohasset/2012/10/water_in_cohasset_crests_over.html)

41. *October 28, Pearl River Patch* – (New Jersey; New York) **Water release from Lake Deforest stopped.** United Water reported it ended the increased water releases from Lake DeForest in New Jersey at the request of the New Jersey Department of Environmental Protection (NJDEP) and with the agreement of the New York State Department of Environmental Conservation (NYSDEC). The NYSDEC requested the release of additional water from Lake DeForest October 28. United Water New York discontinued the release October 27 according to the requests of the NJDEP and NYSDEC. During that time period, the daily flow increased from the permitted 9.75 million gallons to approximately 60 to 80 million gallons. An assemblyman requested the action to mitigate potential flooding expected from Hurricane Sandy. The reservoir was at 99 percent of capacity October 25. The discharge was stopped to allow time for the water to flow downstream before the arrival of Hurricane Sandy. The vice president and general manager of United Water New York, said “Today (October 27), we must allow sufficient time to pass that water through the New Jersey reservoirs before the storm. This is in order to return those reservoirs to the levels they were at before the additional releases began. If not, there is the potential for flooding downstream.”

Source: <http://pearlriver.patch.com/articles/water-releases-from-lake-deforest-stopped>

For another story, see item [18](#)

[[Return to top](#)]



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: <http://www.dhs.gov/IDailyReport>

**Contact Information**

Content and Suggestions:

Send mail to [cikr.productfeedback@hq.dhs.gov](mailto:cikr.productfeedback@hq.dhs.gov) or contact the DHS Daily Report Team at (703)387-2273

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to [support@govdelivery.com](mailto:support@govdelivery.com).

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto:nicc@hq.dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.